PONDURANCE

HANCOCK HEALTH CASE STUDY

How Pondurance Helped Hancock Health Recover from a Major Cybersecurity Incident in 72 Hours

MARCH | 2018

HANCOCK HEALTH CASE STUDY

Hancock Health is an Indiana-based, full-service healthcare network serving Hancock County and the surrounding areas. Its health system includes Hancock Regional Hospital, Hancock Physician Network, and more than 20 other healthcare facilities, such as wellness centers, women's clinics, family practices, and the Sue Ann Wortman Cancer Center. The network has over 1,200 employees, a medical staff of 400, and handles about 160,000 outpatient visits and 90,000 physician visits annually.

Steve Long has been CEO of Hancock Health for nearly four years, and he is incredibly proud of the organization's mission, its exceptional people, and its focus on giving back to the community. The organization strives to put its patients above all else, and as such, security and compliance have always been major focus areas and initiatives that Steve continues to be proud of—especially as they relate to patients. Even though the company had anti-virus software in place, provided employee education about the dangers of email phishing, and regularly monitored and scanned for cybersecurity loopholes and open ports, the organization was hit with a cyber attack on January 11, 2018, that forever changed the way it will view cybersecurity.

THE PROBLEM //

At approximately 9:30 p.m. on Thursday, January 11, Hancock Health's IT team began to notice severe degradation to the system's speed. Within minutes, other departments began contacting IT, indicating that they were seeing pop-ups on their computers that indicated ransomware. Shortly after, Steve was made aware and by 10:30 p.m. that evening, the entire executive team was on site, its attorneys with Hall Render were involved, and the team was ready to tackle the major issue at hand. As a first step, led by the on-call admin, the team physically shut off every single computer across the main campus to prevent the problem from propagating.

Fortunately, Hancock Health had procedures in place that allowed them to switch to a paper system and continue providing top-level care to patients—many who never even realized what was taking place behind the scenes. The team also immediately checked patient safety to ensure no IVs, ventilators, or other physical objects were involved and, very fortunately, none were. In fact, thanks to a thorough audit later conducted, the team learned that the criminals never accessed patient data at all. Soon after the computers were shut off, the team began working in a conference room powered solely by Steve's personal computer, email, and hot spot. Thanks to a referral from the organization's legal counsel, they reached out to Pondurance, an IT security and compliance company, for remediation support.

> ***" ... THEY IMMEDIATELY PROVED THEIR VALUE AND EARNED OUR TRUST DUE TO THEIR IMMENSE EXPERTISE AND GUIDANCE THROUGHOUT THE ENTIRE PROCESS ..."***
>
> *-STEVE LONG, CEO OF HANCOCK HEALTH*

THE SOLUTION //

At 3:30 a.m. on Friday morning, January 12, Pondurance got the call through its Incident Response Hotline, and by 4 a.m. that same morning, Pondurance's experts were were fully engaged. The team immediately got to work to contain the incident. Pondurance found the point of entry for the attack and closed it down, and concurrently deployed a trio of network and host-based appliances, software and active monitoring and hunting. This not only prevented the issue from spreading further, it also served to protect the company from future attacks.

Once the fundamentals were in place, Pondurance provided incident management and crisis leadership to Hancock in order to facilitate the restoration of the production environment.

In addition to spurring into action and engaging the 24/7 security operations center (SOC) team back at Pondurance's headquarters, the team also brought in law enforcement, including the FBI. The law enforcement, combined with Pondurance's deep cybersecurity expertise, were able to help Hancock Health navigate the tricky negotiations with the criminals who were demanding Bitcoin payment in exchange for the decryptions that would allow them to recover the data and systems.

"When we engaged Pondurance, we had no idea who they were or how they could help us, but they immediately proved their value and earned our trust due to their immense expertise and guidance throughout the entire process, but especially in those critical early hours when we had some very important decisions to make," said Steve Long, Hancock Health's CEO.

THE RESULTS //

With Pondurance's expert guidance, Steve and the Hancock Health executive team paid the demanded fee and received the decryption keys at 2 a.m. on Saturday morning—just over two days after the attack. By Sunday night, the organization's electronic medical records were back up, and by Monday morning—three days after the attack—nearly all files were back and systems were almost completely restored. While the exact figure isn't yet known, Steve estimates that this rapid response and restoration process saved the organization hundreds of thousands of dollars.

> ***"WE SIMPLY WOULDN'T HAVE BEEN SUCCESSFUL WITHOUT THEM."***
>
> *-STEVE LONG, CEO OF HANCOCK HEALTH*

Steve shared that in other similar cases, it took weeks—if not months—for healthcare systems to recover. Even though the case is still under investigation, Pondurance, the law enforcement, the legal counsel, and Hancock Health's executives were able to rectify the situation in a timely manner, which was remarkable given the nature of the attack.

"Looking back, we now realize that cybersecurity attacks can happen to any organization at any time," said Steve. *"It's simply not a question of 'if,' but rather 'when.' While we had ample security measures in place, our mindset has changed and we now realize that there are organized criminals out there searching for even the smallest vulnerabilities, and healthcare organizations are incredibly susceptible. Thanks to Pondurance's 24/7 support and expert guidance, we can now fight humans with humans, and are more prepared than ever before. We simply wouldn't have been successful without them."*